PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04B 1/00 — A1

(11) International Publication Number: WO 91/01065

(43) International Publication Date: 24 January 1991 (24.01.91)

(21) International Application Number: PCT/US90/03865

(22) International Filing Date: 10 July 1990 (10.07.90)

(30) Priority data:
378,549 — 10 July 1989 (10.07.89) — US

(60) Parent Application or Grant
(63) Related by Continuation
US — 378,549 (CIP)
Filed on — 10 July 1989 (10.07.89)

(71) Applicant *(for all designated States except US)*: MARTIN MARIETTA ENERGY SYSTEMS, INC. [US/US]; P.O. Box 2009, Oak Ridge, TN 37831-8218 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : MORRISON, Gilbert, Wayne [US/US]; 853 West Woodchase Road, Knoxville, TN 37922 (US). MYHRE, Trygre, Chatham [US/US]; 114 Goldenview Lane, Oak Ridge, TN 37830 (US).

(74) Agents: HOLSOPPLE, Herman, L. et al.; Martin Marietta Energy Systems, Inc., P.O. Box 2009, Oak Ridge, TN 37831-8218 (US).

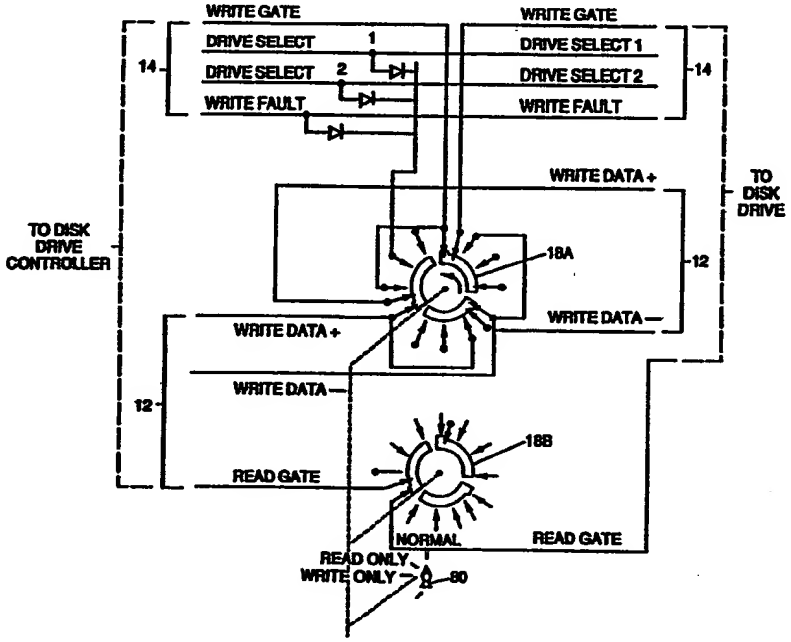
(81) Designated States: AT (European patent), BE (European patent), CA, CH (European patent), DE (European patent)*, DK (European patent), ES (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: LAYERED PROTECTION SYSTEM FOR COMPUTER'S HARD DISK

(57) Abstract

A system (10) and device (18) for controlling access to the hard disk memory portion of a computer on both hardware and software levels, with associated administrative control. A switching device (18) is inserted in the wiring between the hard disk controller and the hard disk (32), requiring the application of a key (34) or other suitable electronic or digital access means for operation of the switch allowing an unprotected mode, a mode wherein a disk (24) in a protected disk drive may be read from but not written to; a mode wherein a disk (24) in a protected disk drive may be written to but not read from and a mode wherein a disk (24) in a disk drive may neither be read from nor written to and a software program verifying the functioning of the hardware and providing means to detect an attempted access of a protected drive and maintaining a status log for security audit purposes. The key (34) and the software program being administratively controlled.



* See back of page

DESIGNATIONS OF "DE"

Until further notice, any designation of "DE" in any international application whose international filing date is prior to October 3, 1990, shall have effect in the territory of the Federal Republic of Germany with the exception of the territory of the former German Democratic Republic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MC	Monaco
AU	Australia	FI	Finland	MG	Madagascar
BB	Barbados	FR	France	ML	Mali
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Fasso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GR	Greece	NL	Netherlands
BJ	Benin	HU	Hungary	NO	Norway
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	SD	Sudan
CF	Central African Republic	KP	Democratic People's Republic of Korea	SE	Sweden
CG	Congo			SN	Senegal
CH	Switzerland	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
DE	Germany, Federal Republic of	LK	Sri Lanka	TG	Togo
DK	Denmark	LU	Luxembourg	US	United States of America

LAYERED PROTECTION SYSTEM FOR COMPUTER'S HARD DISK

This application in part discloses and claims subject matter disclosed in our earlier filed pending application, Serial Number 07/378,549, filed July 10, 1989.

The U.S. Government has rights in this invention pursuant to Contract No. DE-AC05-840R21400 awarded by the U.S. Department of Energy contract with Martin Marietta Energy Systems, Inc.

Technical Field

This invention relates to the field of computer disk security and more particularly concerns a multilevel system and device for preventing unauthorized access to such a computer disk.

Background Art

In establishments using proprietary or classified information, especially in the government and military environments, microcomputers equipped with nonremovable "hard" disks are approved for handling sensitive information only in secured areas because sensitive information could be stored intentionally or inadvertently on the nonremovable "hard" disks. As a result, the sensitive information could be obtained by unauthorized individuals. Also, information that is legitimately stored on these nonremovable "hard" disks needs protection from inadvertent erasure or alteration. The effort of maintaining computers in an environment free from such undesirable occurrences as these naturally hampers productivity. However, productivity could be

significantly increased if microcomputer's central processor could be accessed while verifiably preventing unauthorized access to the information stored on the computer's disk drives. Similar problems could also exist for computer users in private industry.

The prior art made of record in the parent case is herein incorporated by reference. While some of the above referenced art addresses the problem of controlling access to the computer, the prior art relies on physical obstructions to the external openings to the drive bays or to keyed "on-off" switches. The art does not offer or suggest a system that simultaneously offers access to the processing capabilities of the computer while verifiably preventing access to the information stored in the protected disk drives.

Accordingly, it is an object of this invention to provide a multilayered system incorporating hardware and software which verifiably prevents undesirable access to a computer's hard disk memory while allowing an operator to use the computer's central processor.

It is another object of the present invention to provide a multilayered system incorporating hardware and software which also prevents undesirable access to a computer's floppy disk drive(s) if such protection is warranted.

It is another object of this invention to provide a multilayered security system which maintains a status log of all protected disk checks and activities for purposes of routine security audit checks.

It is another object of this invention to provide a multilayered security system which prevents "virus" contamination of protected drives.

Other objects and advantages over the prior art will become apparent to those skilled in the art upon reading the detailed description together with the drawings as described as follows.

Disclosure of the Invention

In accordance with various features of the present invention, a layered protection system for a computer disk is provided wherein both read and write access to the hard disk of a computer are controlled and can be prevented on multiple cooperating levels. The layered protection system for a computer disk includes a hardware layer, wherein certain of the electrical wires which connect the computer to the disk controller are physically interrupted with a switching device inserted therebetween to reestablish the electrical connections only under controlled conditions.

Maintaining administrative control of the key for the security switch comprises another cooperating level of controlling the access to the hard disk memory. Within the multilevel protection program of the preferred embodiment of the present invention, four operating modes are established. The first such operating mode is a "NORMAL" mode, wherein an operator can both read from and write to the hard disk memory of a computer. The second is a "READ ONLY" mode, wherein an operator can read from the hard disk but cannot write to it. The third mode is for "WRITE ONLY", wherein an operator can write data into the hard disk memory of a computer but cannot read from it. Finally, there is a "NEITHER" mode, wherein an operator can neither read from nor write to the hard disk memory, but can still utilize all the other functions of the affected computer.

The layered protection system also includes a software layer that verifies that the hardware is both functioning and in use. This software "locks up" the system in the event of a failure on the part of the hardware. The software also initiates and maintains a status log for security audit purposes. Administrative controls require the computer to be started with a "boot"

disk which contains the software layer. The software functions as a "Terminate and Stay Resident" (TSR) program. This allows the software to verify that the hardware is functioning and prevent unauthorized access to the hard disk while the operator is using the computer. When the computer user is finished working in a classified environment the software is again utilized to verify that the protected disks have not been written to and to update the security audit status log.

Brief Description of the Drawings

The above mentioned features of the invention will become more clearly understood from the following detailed description of the invention read together with the drawings in which:

Figures 1A, 1B, and 1C are pictorial views of the components of an access restricting system.

Figure 2 is a pictorial diagram of a typical switching device constructed in accordance with various features of the present invention.

Figure 3 is a general schematic diagram of the electrical system of the access restricting system pictured in Figure 1.

Figure 4 is a detailed schematic diagram of the electrical system of the present invention.

Figure 5 illustrates a flow diagram of the operational steps of the software layer of the invention during the start-up in which the software verifies that the hardware is functioning prior to allowing the user access to the computer.

Figure 6 illustrates a flow diagram of operational steps of the software in TSR mode and the steps in the "QUIT" portion of the software that verifies that no unauthorized changes have been made to the protected disks during the period of the operator's use.

Best Mode For Carrying Out The Invention

A layered protection system for a computer disk is illustrated pictorially in Figures 1A, 1B, and 1C. Figure 1A illustrates a key 34 and a lock means 28 that cooperate with a security switch 18 illustrated in Figure 1B. These elements are shown as representing the "hardware" portion of the layered protection system for a computer disk.

The mechanical components of the lock and switch means are well known in the art and are typical of the multiple-pole, multiple-throw locking electrical switch that can be obtained "off the shelve". Of importance is the manner, described herein, that the locking electrical switch is interfaced with the computer. It will be recognized by those skilled in the art that the switch 18, with its key 34 and lock 28, can also be installed directly within the computer 30 or within a housing for fixed disk drive. The choice of location will depend upon the particular installation play for the present invention, the important feature being to interrupt the communication between the hard disk and the computer.

A perspective view of a typical embodiment of this hardware portion of the administrative control level is shown at 22 in Figure 2. This includes a housing 20 for the enclosure of the switch 18 (not shown in this figure), this switch accepting the aforementioned key 34 and lock 28. Illustrated are the various electrical cables 12, 14 that connect the switch with a disk drive controller and the disk drive itself.

While a mechanical key and lock have been described and illustrated, it will of course be understood that an electronic or a digital security switch, which are well known in the art, will also provide a suitable means for preventing or allowing access.

A general schematic diagram of the system of the

present invention is illustrated in Figure 3. Here it can be seen that the cables 12, 14 are used to connect the hardware portion 22 of the administrative control level to a drive controller in a computer 30, or it can be a separate unit if desired. The switch 18 within the enclosure 20 is illustrated for convenience as a double-pole switch; however, as illustrated in both Figure 1B and Figure 4, this is a multi-pole, multi-throw switch. As discussed in greater detail hereinafter, only a portion of the electrical leads between the drive controller and the disk drive needs to be interrupted by the switch. The remaining electrical leads are designated at 40 in Figure 3. These leads 40 can either bypass the housing 20 or can be routed therethrough.

A detailed schematic diagram of the hardware system of the administrative control of the present invention is shown in Figure 4. As stated above, the switch 18 is typically a multi-pole, multi-throw type. The switch has an indicator 80 which will indicate the position of the switch in the following positions, which are discussed below: "NORMAL", "READ ONLY", "WRITE ONLY", AND "NEITHER". In the preferred embodiment, the key-out position, i.e., the only position in which the key can be removed, is the neither position.

The specific wires to be interrupted by being connected to switch 18 include the wires to at least a "Drive Select", a "Write Gate", a "Write Enable", a "Read Gate", and two "Write Data" lines, in which the total travel distance added by the switching device 22 and input and output leads for data transmission between the computer 30 and the hard disk 32 drive are preferably of equal length and preferably no longer than five feet, in order to maintain correct timing for data transmitted through the switching device 22.

Referring next to the schematic diagram of Figure 4, it will be observed that in the "NORMAL" operating

position, the hard disk memory can be both written to and read from so that the full and complete capabilities of the computer and its associated hard disk memory are available to the operator. When key 34 is inserted and switch 18 operated to the "READ ONLY" mode, the line labelled "WRITE DATA +" is open-circuited by contacts 1 and 2, the line labelled "WRITE DATA -" is open-circuited by contacts 3 and 4 and the "WRITE GATE" line is open-circuited between contacts 7 and 9 of switch 18A, precluding any possibility of writing to (storing data on) the hard disk memory. In the "WRITE ONLY" position of the switch 18, the "READ GATE" lines are open-circuited by contacts 5 and 6 of section B of switch 18, as shown, so that no data stored on the hard disk memory can be read. In the "NEITHER" position of the switch, the three lines labeled "WRITE FAULT", "DRIVE SELECT 1", and "DRIVE SELECT 2" are disabled by being electrically connected through contacts 7 and 8 of switch 18A to the "WRITE GATE" line through isolating diodes 38.

It will be recognized by those skilled in the art that this is necessary to avoid the pick-up or generation of noise in the open leads. Simultaneously, the "WRITE GATE" line is again open-circuited between contacts 7 and 9 of switch 18A as described above.

Of course, it will also be apparent to those skilled in the art that, in another embodiment of the present invention, existing cables to a computer to be modified with the present invention can be replaced by wholly fabricated replacement cables with the switching device of the present invention manufactured in place as an integral part of such replacement cables. Furthermore, as has already been mentioned, security switch 18 or its equivalent can be mounted or attached in some location other than that exemplified, such as directly on the circuit board of the controller or disk drive, for instance.

In the preferred embodiment, the software layer of the present invention is utilized to verify that the hardware is functioning to disable the disk controller. This layer verifies that a protected disk is indeed protected.

The flow diagrams depicted in Figs. 6 and 7 illustrate the operation of the software system in the preferred embodiment.

While the flow diagrams can be easily read by those skilled in the art, the system operation based on the rules depicted in the diagrams will be discussed. However, it will be noted that the flow diagrams depict preferred operational embodiments. The specific references are enclosed as examples only, and are not intended to limit the scope of the invention.

Initially, the operator disengages the computer from any and all unclassified connections, e.g. a network, and the key 34 is removed from the switch 18 as indicated at 120 "configure for protective mode". The operator then inserts the boot disk which contains the software level of the security system and turns the computer on. The "autoexec.bat" file contained on the boot disk activates the "protect" program. The "protect" program can be initiated to protect all drives, all drives except a given drive, or any specifically designated drive(s). For purposes of illustration the flow diagram designates drive "n" as any given drive.

The prpgram then initiates the status log record at 125. The audit record status is set at zero (0) at 126 and the keyboard is locked at 127. While the audit record status can be designated as any given set of values, in the preferred, illustrated embodiment the values shown in Table 1 are used.

Value	Meaning
0	Start-up not completed; Quit not run.
1	Failure during start-up.
2	Start-up successfully run; Quit not run.
3	Write attempt to protected drive during operation.
4	Test failure during operation.
5	Test failure during running Quit.
9	Quit successfully run at session end; there were no anomalies.

Table I

The system then identifies the first protected drive and determines if that drive is indeed protected at 130. In the event that the drive is not protected, this result is displayed at 135 and the audit record status is updated to one (1). The operator is prompted to reconfigure for protected mode and instructed that the software will reboot the system in a preselected amount of time. In the illustrated preferred embodiment the system reboots in about fifteen (15) seconds. This causes the "Protect" program to be reactivated at 124. If drive "n" passes the initial test at 130, that result is displayed and the program repeats 130 for each protected drive. When the last protected drive passes the initial test at 130, the audit record status is updated to two (2) and the display notifies the user that the test of the protected drives is complete. The boot record, the File Allocation Table (FAT) and the checksums of each protected drive is copied to the boot disk at 140. The protect program enters a "terminate and stay resident" (TSR) mode and the key board is unlocked at 145. Those skilled in the art will recognize that the locking of the keyboard at 127 and the unlocking of the keyboard at 145 is an internal feature of the software and is not to be confused with the locking electrical switch described above.

At this point the operator has complete use of the

processing capabilities of the computer. The TSR protect program continually monitors at 150 any attempt to write to a protected disk. When such an attempt is detected at 155, the operator is prompted to reinsert the boot disk, the audit record status is updated to 3. The operator is prompted to reconfigure for protected mode and instructed that the software will reboot the system in a preselected amount of time. In the illustrated preferred embodiment the system reboots in about fifteen (15) seconds. This reinitiates the "Protect" program at 124.

When the user is finished operating in a classified environment the user must reinsert the boot disk and execute the "Quit" program. The "Quit" program compares the current boot record, the current FAT, and the current checksums with those saved on the boot disk. If the records are the same, the audit record status is updated to nine (9). The system locks the keyboard and displays the test results at 164. In the preferred embodiment, the system displays:

> Checksum test complete. Sanitize the system; be sure to power down and remove all classified materials.

At this time the system must be powered down.

If the current records are different than the records saved on the boot disk, the audit record status is updated to five (5). The keyboard is locked and the system notifies the user of the failure. In the preferred embodiment, the system displays:

> FAILURE: Drive "n" failed the checksum [boot, or FAT] test. CONTACT YOUR DIVISION COMPUTER SECURITY OFFICER (CSO) IMMEDIATELY.

At this time the system must be powered down.

From the foregoing description, it will be recognized by those skilled in the art that a layered protection system for a computer disk offering advantages over the prior art has been provided. Specifically, the

layered protection system for a computer disk provides a multilayered system incorporating hardware and software which verifiably prevents undesirable access to a computer's hard disk, and if warranted the system further prevents undesirable access to a computer's floppy disk drive(s), while allowing an operator to use the computer's central processor. The system maintains a status log of all protected disk checks and activities for purposes of routine security audit checks. It will be obvious to those skilled in the art that while in the protected mode the system also prevents "virus" contamination of protected drives.

While a preferred embodiment has been shown and described, it will be understood that it is not intended to limit the disclosure, but rather it is intended to cover all modifications and alternate methods falling within the spirit and the scope of the invention as defined in the appended claims.

Having thus described the aforementioned invention, We claim:

1. A layered protection system for controlling access to a hard disk memory system from a disk drive controller of a computer system, which comprises:

a switch means connected between said disk drive controller and said disk memory system, said switch means having contact means connected to selected electrical circuits joining said disk drive controller to said disk memory system, and having means for selectively accessing selected of said contact means;

lock means associated with said switch means to selectively inhibit access to a protected disk drive's operation via said switch means; and

means for selectively operating said lock means for administrative control of accessing said disk memory system from said disk drive controller.

2. The layered protection system of Claim 1 wherein said switch means and said lock means associated with said switch means are mounted in a housing separate from said disk drive controller and said hard disk memory system.

3. The layered protection system of Claim 1 wherein said switch means and said lock means associated with said switch means are mounted on the same printed circuit board as other electronic components of said disk drive controller.

4. The layered protection system of Claim 1 wherein said switch means and said lock means associated with said switch means are mounted in a housing containing said hard disk memory system.

5. The layered protection system of Claim 1 wherein said switch means is a rotary switch member having a plurality of selected rotary positions whereby said means for accessing said contacts is a rotary shaft carrying moving contacts whereby, at a given rotary position, a selected number of said rotary contacts interact with a selected number of said contact means for selectively connecting selective of said electrical circuits joining said hard disk memory system and said disk drive controller.

6. The layered protection system of Claim 5 wherein said plurality of rotary positions provides for at least operation in an unprotected mode wherein a disk in said protected disk drive may be read from and written to; operation in a mode allowing a disk in said protected disk drive to be read from but not written to; operation in a mode allowing a disk in said protected disk drive to be written to but not read from and operation in a mode wherein a disk in said disk drive can neither be read from nor written to.

7. A layered protection system for controlling access to a computer's disk memory system from a disk drive controller of a computer system, which comprises:

a switch means connected between said disk drive controller and said disk memory system, said switch means having contact means connected to selected electrical circuits joining said disk drive controller to said disk memory system, and having means for selectively accessing selected of said contact means;

lock means associated with said switch means to selectively inhibit access to a protected disk drive's operation via said switch means;

means for selectively operating said lock means for administrative control of accessing said disk memory system from said disk drive controller;

hardware verification means whereby said switch means is tested to insure that said switch means is selectively operated to disallow access to said protected disk drive and is operable;

protected disk drive selection means for selectively controlling which said disk drive is to be protected; and

protected disk drive identification means for determining which of said computer's said disks are protected.

8. The layered protection system of Claim 7 wherein said layered system further comprises:

status audit means whereby security status of said protected disks is recorded for security audit purposes.

9. The layered protection system of Claim 7 wherein said layered system further comprises:

access inhibiting means whereby unauthorized attempts to access said protected disk drive are obstructed.

10. The layered protection system of Claim 7 wherein said layered system further comprises:

non-access verification means whereby said layered protection system can verify that no access to said protected disk drives has been allowed.

11. A layered protection system for controlling access to a computer's disk memory system from a disk drive controller of a computer system, which comprises:

a switch means connected between said disk drive controller and said disk memory system, said switch means

having contact means connected to selected electrical circuits joining said disk drive controller to said disk memory system, and having means for selectively accessing selected of said contact means;

lock means associated with said switch means to selectively inhibit access to a protected disk drive's operation via said switch means;

means for selectively operating said lock means for administrative control of accessing said disk memory system from said disk drive controller;

hardware verification means whereby said switch means is tested to insure that said switch means is selectively operated to disallow access to said protected disk drive and is operable;

protected disk drive selection means for selectively controlling which said disk drive is to be protected;

protected disk drive identification means for determining which of said computer's said disk drives are protected;

status audit means whereby security status of said protected disk drives is recorded for security audit purposes;

access inhibiting means whereby unauthorized attempts to access said protected disk drive are obstructed; and

non-access verification means whereby said layered protection system can verify that no access to said protected disk drives has been allowed.

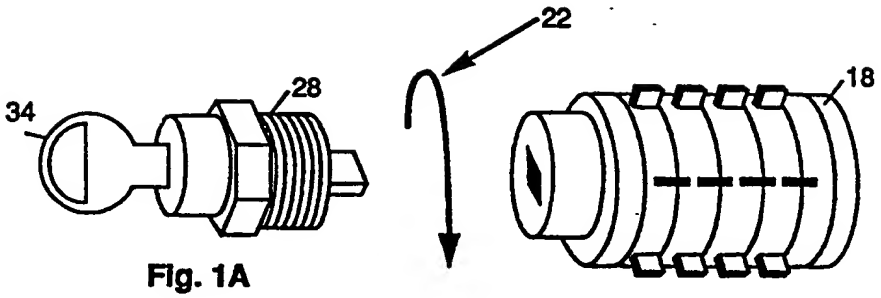


Fig. 1A

Fig. 1B

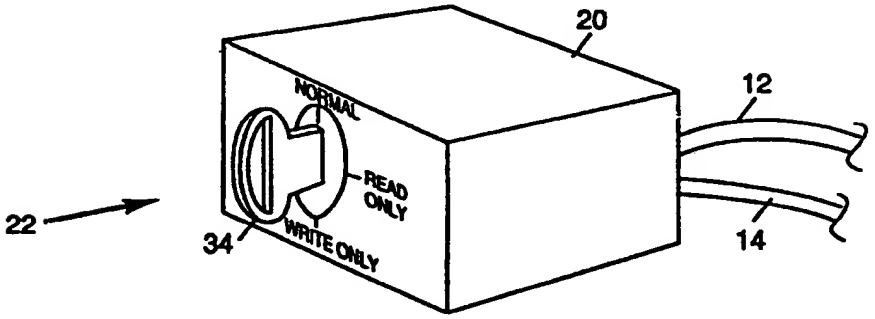


Fig. 2

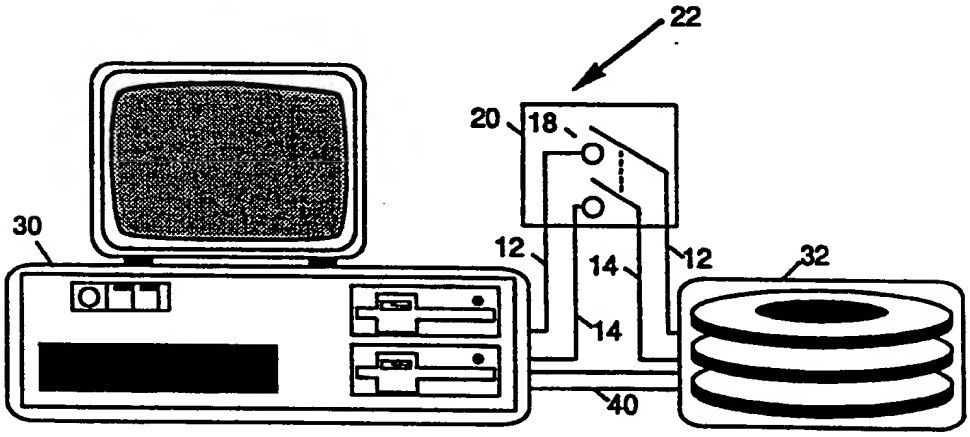


Fig. 3

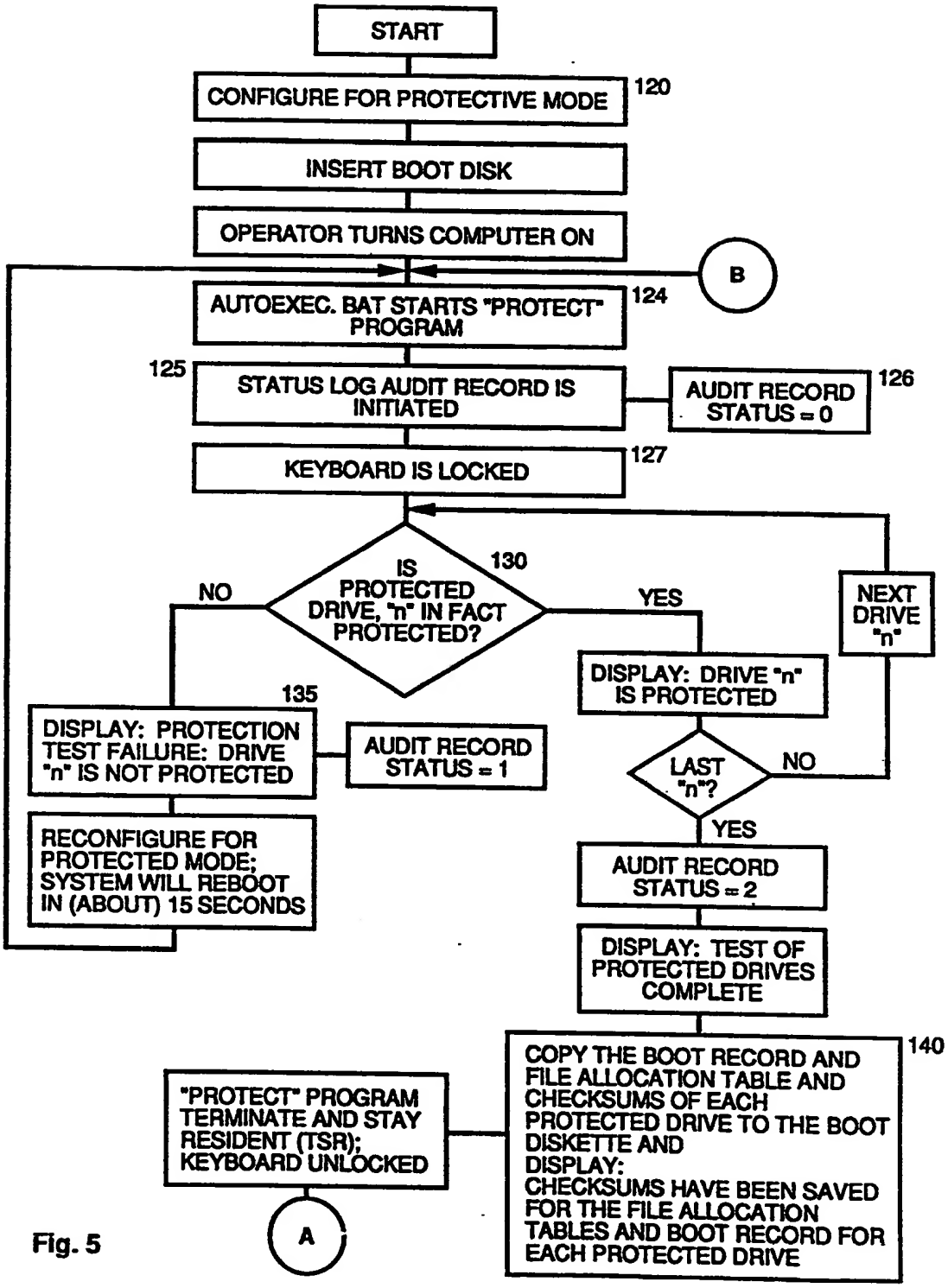

START
CONFIGURE FOR PROTECTIVE MODE
120
INSERT BOOT DISK
OPERATOR TURNS COMPUTER ON
B
AUTOEXEC. BAT STARTS "PROTECT" PROGRAM
124
125
STATUS LOG AUDIT RECORD IS INITIATED
AUDIT RECORD STATUS = 0
126
KEYBOARD IS LOCKED
127
IS PROTECTED DRIVE, "n" IN FACT PROTECTED?
130
NO
YES
NEXT DRIVE "n"
DISPLAY: DRIVE "n" IS PROTECTED
135
DISPLAY: PROTECTION TEST FAILURE: DRIVE "n" IS NOT PROTECTED
AUDIT RECORD STATUS = 1
LAST "n"?
NO
YES
RECONFIGURE FOR PROTECTED MODE; SYSTEM WILL REBOOT IN (ABOUT) 15 SECONDS
AUDIT RECORD STATUS = 2
DISPLAY: TEST OF PROTECTED DRIVES COMPLETE
140
COPY THE BOOT RECORD AND FILE ALLOCATION TABLE AND CHECKSUMS OF EACH PROTECTED DRIVE TO THE BOOT DISKETTE AND DISPLAY: CHECKSUMS HAVE BEEN SAVED FOR THE FILE ALLOCATION TABLES AND BOOT RECORD FOR EACH PROTECTED DRIVE
"PROTECT" PROGRAM TERMINATE AND STAY RESIDENT (TSR); KEYBOARD UNLOCKED
A

Fig. 5

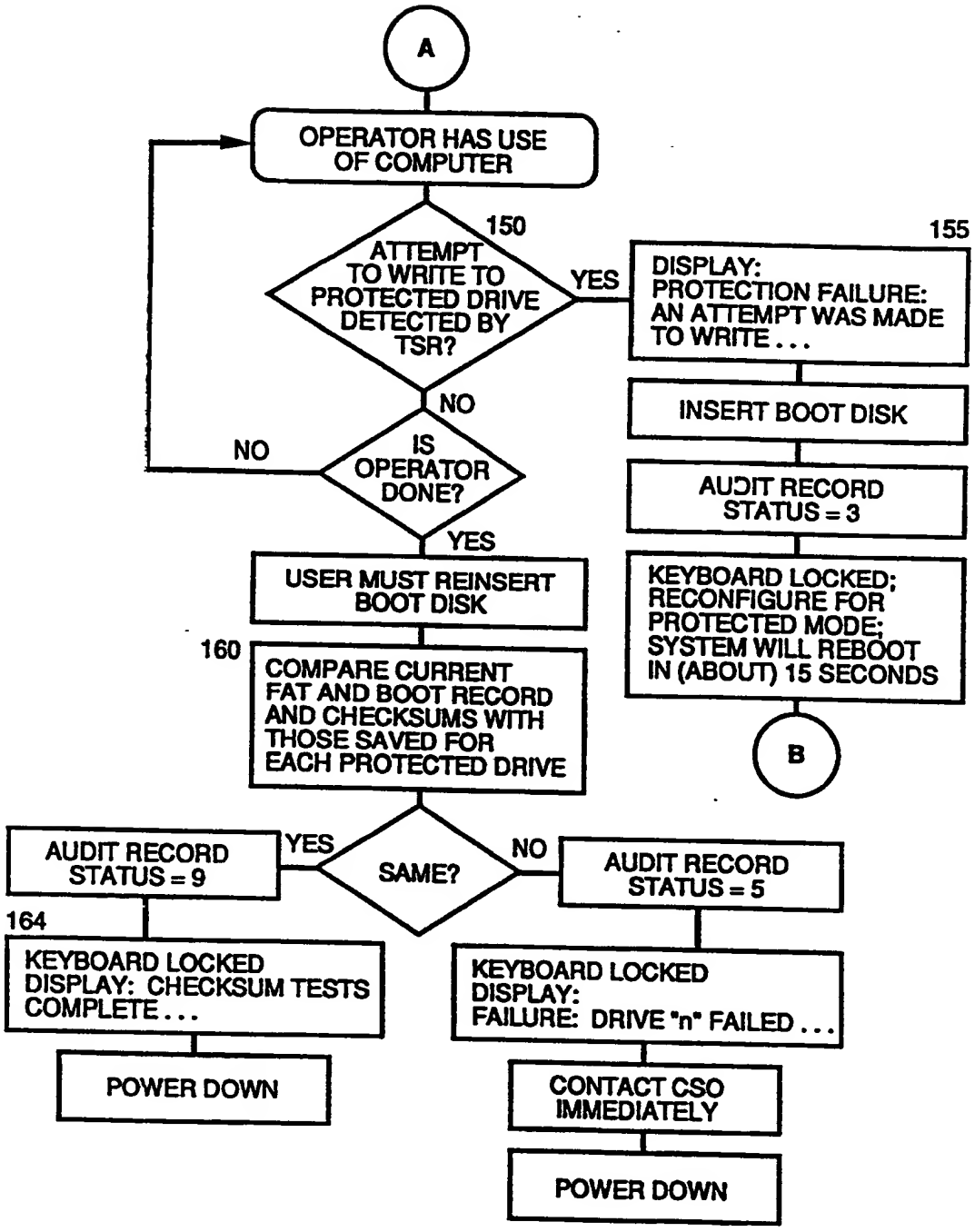

A
OPERATOR HAS USE OF COMPUTER
150
ATTEMPT TO WRITE TO PROTECTED DRIVE DETECTED BY TSR?
YES
155
DISPLAY: PROTECTION FAILURE: AN ATTEMPT WAS MADE TO WRITE . . .
INSERT BOOT DISK
AUDIT RECORD STATUS = 3
KEYBOARD LOCKED; RECONFIGURE FOR PROTECTED MODE; SYSTEM WILL REBOOT IN (ABOUT) 15 SECONDS
B
NO
IS OPERATOR DONE?
NO
YES
USER MUST REINSERT BOOT DISK
160
COMPARE CURRENT FAT AND BOOT RECORD AND CHECKSUMS WITH THOSE SAVED FOR EACH PROTECTED DRIVE
AUDIT RECORD STATUS = 9
YES
SAME?
NO
AUDIT RECORD STATUS = 5
164
KEYBOARD LOCKED DISPLAY: CHECKSUM TESTS COMPLETE . . .
KEYBOARD LOCKED DISPLAY: FAILURE: DRIVE "n" FAILED . . .
POWER DOWN
CONTACT CSO IMMEDIATELY
POWER DOWN

Fig. 6

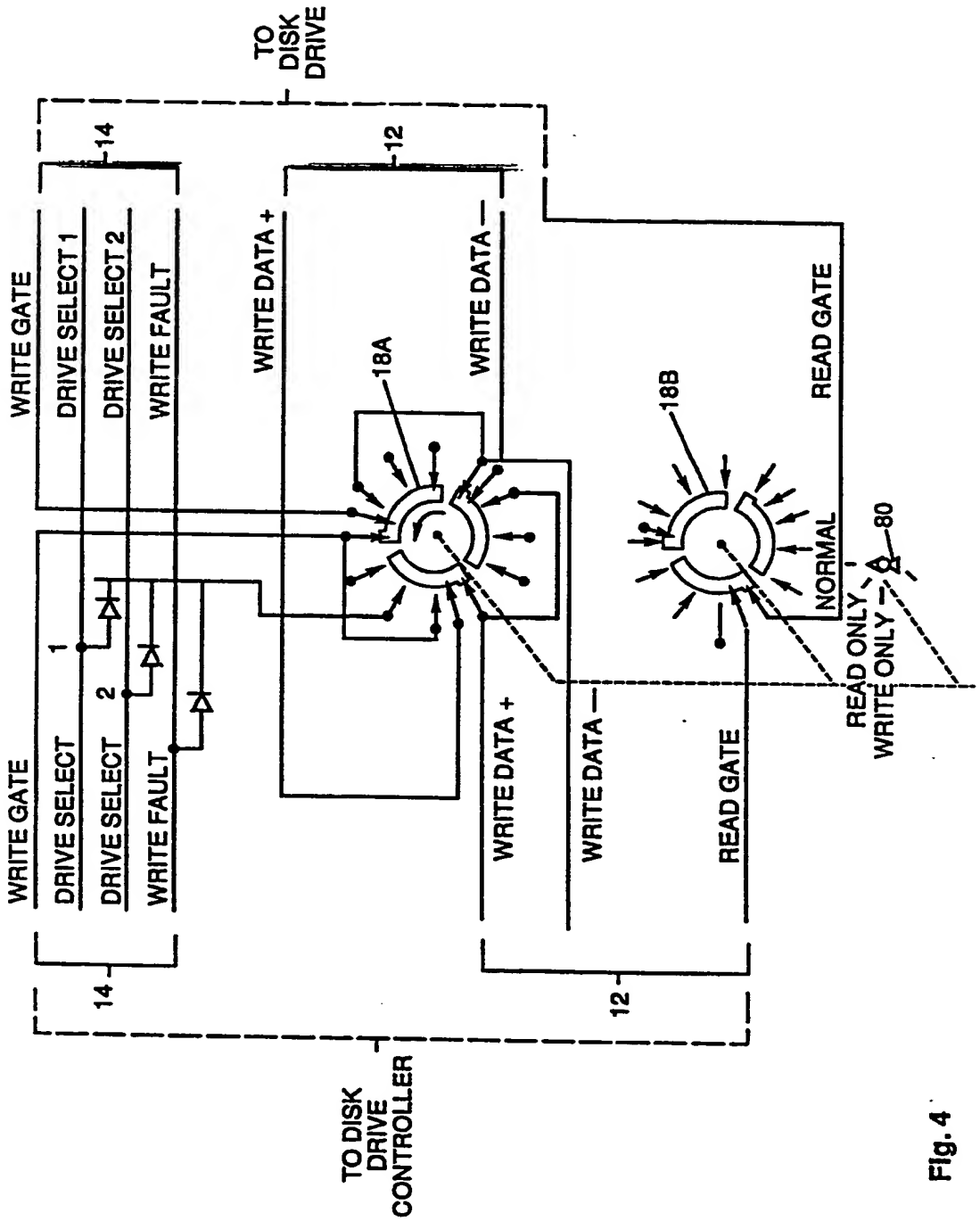

TO DISK DRIVE
14
12
WRITE GATE
DRIVE SELECT 1
DRIVE SELECT 2
WRITE FAULT
WRITE DATA +
WRITE DATA —
18A
18B
READ GATE
NORMAL
80
READ ONLY
WRITE ONLY
1
2
WRITE GATE
DRIVE SELECT
DRIVE SELECT
WRITE FAULT
WRITE DATA +
WRITE DATA —
READ GATE
14
12
TO DISK DRIVE CONTROLLER

Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No PCT/US90/03865

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) 3

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. CL. (5): H04B 1/00

U.S. CL: 340/825.00; 307/112; 70/271

II. FIELDS SEARCHED

Minimum Documentation Searched 4

Classification System	Classification Symbols
U.S.	340/825; 360/92,97.01,97.02,98.01,98.05,133,137;364/709.01, 709.05 365/195;361/380,393,395;200/43.04,43.08,43.11,43.22,50B, 116; 70/14,58,263,271, 307/112,142

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched 5

III. DOCUMENTS CONSIDERED TO BE RELEVANT 14

Category *	Citation of Document, 16 with indication, where appropriate, of the relevant passages 17	Relevant to Claim No. 18
A,P	US, A, 4,907,111 (DERMAN) 06 March 1990 See Figures 4,5, and 8; column 3 and 4	1-11
A,P	US, A, 4,890,006 (HUANG) 26 December 1989 See Figures 1,6, and 9-11; columns 2-3.	1-11
A	US, A, 4,685,312 (LAKOSKI ET AL.) 11 August 1987 See Figure 8; column 6, lines 39-66.	1-11
A	US, A, 4,634,822 (GOEKE) 06 January 1987 See Figures 3,6, and 14; columns 1,2,10	1-11

* Special categories of cited documents: 15

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search 2	Date of Mailing of this International Search Report 2
30 JULY 1990	19 NOV 1990
International Searching Authority 1	Signature of Authorized Officer 20
ISA/US	NGOC-HO NGUYEN INTERNATIONAL DIVISION DERVIS MAGISTRE

Form PCT/ISA/210 (second sheet) (May 1986)